UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/602,696	06/25/2003	Makoto Aikawa	501.42780X00	1583

24956 7590 08/10/2007

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
GERGISO, TECHANE	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
08/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/602,696	AIKAWA ET AL.	
	Examiner	Art Unit	
	Techane J. Gergiso T-C	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05/10/2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3, 5, and 8* is/are rejected.

7)☒ Claim(s) *2, 4, 6, 7 and 9* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a Final Office Action in response to the applicant's communication filed on May 10, 2007.

2. Claims 1-9 have been examined and are pending.

Response to Arguments

3. Applicant's arguments filed May 10, 2007have been fully considered but they are not persuasive.

4. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

5. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e.,

Page 15: paragraph 1: Also **according to the present invention**, the arithmetic processing unit updates the transfer key identifier and the transfer key **by performing encryption using the update key on the basis of common-key cryptography**. Furthermore, according to the present invention, the arithmetic processing unit updates the value data **by performing encryption using the transfer key on the basis of the common-key cryptography**. The prior art does not teach or suggest all of these features.) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations

from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

6. The applicant also argues "Guthery does not teach or suggest a transfer key identifier that judges whether the transfer key is newer or older in accordance with a value of the transfer key identifier, an update key that updates the transfer key, and an upper limit of the transfer key identifier that represents an upper limit of the transfer key that can be stored by the smart card." However, the examiner **disagrees** because at least figure 10 and 11 of Guthery shows the evaluation to judge whether the authentication vector is modified or unmodified to keep the modified authentication vector and figure the authentication vector tracks which identities are currently authenticated by the card at any time.

7. Therefor, the applicant's argument is not persuasive to overcome the prior arts in record to place independent claims 1, 3, 5 and 8 in condition for allowance.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1-9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

10. Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999).

The term "**update**" in claim 1-9 are used by the claim to likely mean "**encryption**", while the accepted meaning is **"To change a system or a data file to make it more current." (See Microsoft Computer Dictionary).** The term is indefinite because the specification does not clearly redefine the term.

The term "**judge** " in claim 1-9 are used by the claim to likely mean "verification", while the accepted ordinary meaning is **"To form an opinion or estimation after careful consideration." (See The American Heritage Dictionary).** The term is indefinite because the specification does not clearly redefine the term.

11. The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

Fore example **the third limitation in claim 4 reads and it is not clear to what extent it determines the scope of the claim**:

" wherein if command data which requests update of the transfer key, and which stores second encrypted data and second digital signature data, is received, said arithmetic processing unit first checks the second digital signature data by use of the second public key on the basis of public-key cryptography, next decrypts the second encrypted data by use of the secret key on the basis of public-key cryptography to extract first data and second data, and lastly if a value of the first data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updates a value of the transfer key identifier to a value of the first data, and updates a value of the transfer key to a value of the second data;"

The limitations in the claims are required to be rewritten to provide in a clear and precise language to determine the scope and boundaries of the claimed invention.

See MPEP

2173 Claims Must Particularly Point Out and Distinctly Claim the Invention

The primary purpose of this requirement of definiteness of claim language is to ensure that the scope of the claims is clear so the public is informed of the boundaries of what constitutes infringement of the patent. A secondary purpose is to provide a clear measure of what applicants regard as the invention so that it can be determined whether the claimed invention meets all the criteria for patentability and whether the specification meets the criteria of 35 U.S.C. 112, first paragraph with respect to the claimed invention.

and

2173.02 [R-3] Clarity and Precision

The examiner's focus during examination of claims for compliance with the requirement for definiteness of 35 U.S.C. 112, second paragraph, is whether the claim meets the threshold requirements of clarity and precision, not whether more suitable language or modes of expression are available. When the examiner is satisfied that patentable subject matter is disclosed, and it is apparent to the examiner that the claims are directed to such patentable subject matter, he or she should allow claims which define the patentable subject matter with a reasonable degree of particularity and distinctness. Some latitude in the manner of expression and the aptness of terms should be permitted even though the claim language is not as precise as the examiner might desire. Examiners are encouraged to suggest claim language to applicants to improve the clarity or precision of the language used, but should not reject claims or insist on their own preferences if other modes of expression selected by applicants satisfy the statutory requirement.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 1, 3, 5, and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guthery (US Pat No: 6, 779, 113) in view of Akiyama et al. (hereinafter referred to as Akiyama, US Pat. No.: 6, 018, 717).

As per claim 1:

Guthery disclose a smart card (figure 2: 26; IC Card), comprising:

A communication unit to communicate with the outside (figure 2: 50; Reader Interface);

An information accumulating unit to accumulate data and a program (figure 2: 54; RAM; 56);

An arithmetic processing unit to perform information processing (figure 2: 52 CPU, Cryptography Accelerator; 62);

Wherein said information accumulating unit stores value data, a transfer key that updates the value data, a transfer key identifier that judges whether the transfer key is newer or older in accordance with a value of the transfer key identifier, an update key that update the transfer key, and an upper limit of the transfer key identifier that represents an upper limit of the transfer key identifier that can be stored by the smart card (Column 5: lines 27-42; Column 6: lines 60-67; column 7: line 1-5; column 12: lines 1-25);

Wherein said arithmetic processing unit updates the transfer key identifier and the transfer key by performing encryption using the update key on the basis of common-key cryptography (column 7: lines 39-45); and

Wherein said arithmetic processing unit then updates the value data by performing encryption using the transfer key on the basis of the common-key cryptography (column 7: lines 39-45).

Guthery does not disclose update value data. Akiyama, in analogous art, however, discloses updating transaction and update value data (Figure 15: IC card ledger file). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Guthery to include updating transaction and update

value data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an enhanced security of an electronic cashless transaction system, thereby allowing versatile uses of an IC card as an ultimate medium for commercial transactions in general as suggested by Akiyama in (column 4: lines 43-48).

As per claim 3:

Guthery disclose a smart card, comprising:

A communication unit to communicate with the outside (figure 2: 26; IC Card);

An information accumulating unit to accumulate data and a program (figure 2: 54; RAM; 56); and

An arithmetic processing unit to perform information processing (figure 2: 52 CPU, Cryptography Accelerator; 62);

Wherein said information accumulating unit stores value data, a transfer key that updates the value data, a transfer key identifier that judges whether the transfer key is newer or older in accordance with a value of the transfer key identifier, a first public key certificate including a first public key, which is used to update the transfer key, a secret key corresponding to the first public key, and an upper limit of transfer key identifier that represents an upper limit of the transfer key identifier which can be stored by the smart card (Column 5: lines 27-42; Column 6: lines 60-67; column 7: line 1-5; column 12: lines 1-25);

Wherein said arithmetic processing unit updates the transfer key identifier and the transfer key by performing encryption using the first public key certificate and the secret key on the basis of public-key cryptography (column 7: lines 39-45); and

Wherein said arithmetic processing unit then updates the value data by performing encryption using the transfer key on the basis of common-key cryptography (column 7: lines 39-45).

Guthery does not disclose update value data. Akiyama, in analogous art, however, discloses updating transaction and update value data (Figure 15: IC card ledger file). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Guthery to include updating transaction and update value data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an enhanced security of an electronic cashless transaction system, thereby allowing versatile uses of an IC card as an ultimate medium for commercial transactions in general as suggested by Akiyama in (column 4: lines 43-48).

As per claim 5:

Guthery disclose a smart card, comprising:

A communication unit to communicate with the outside (figure 2: 26; IC Card);

An information accumulating unit to accumulate data and a program (figure 2: 54; RAM; 56); and

An arithmetic processing unit to perform information processing (figure 2: 52 CPU, Cryptography Accelerator; 62);

Wherein said information accumulating unit stores value data, a transfer key that updates the value data, a transfer key identifier that judges whether the transfer key is newer or older in accordance with a value of the transfer key identifier, an update key that updates the transfer key, an update key identifier that judges whether the update key is newer or older in accordance with a value of the update key identifier, a first public key certificate including a first public key, which updates the transfer key, a secret key corresponding to the first public key, and an upper limit of transfer key identifier that represents an upper limit of the transfer key identifier which can be stored by the smart card (Column 5: lines 27-42; Column 6: lines 60-67; column 7: line 1-5; column 12: lines 1-25);

Wherein said arithmetic processing unit updates the transfer key by use of the update key on the basis of common-key cryptography, or updates the transfer key by use of the first public key certificate and the secret key on the basis of common-key cryptography (column 7: lines 39-45); and

Wherein said arithmetic processing unit then updates the value data by performing encryption using the transfer key on the basis of the common-key cryptography (column 7: lines 39-45).

Guthery does not disclose update value data. Akiyama, in analogous art, however, discloses updating transaction and update value data (Figure 15: IC card ledger file). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention

was made to modify the system disclosed by Guthery to include updating transaction and update value data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an enhanced security of an electronic cashless transaction system, thereby allowing versatile uses of an IC card as an ultimate medium for commercial transactions in general as suggested by Akiyama in (column 4: lines 43-48).

As per claim 8:

Guthery disclose a smart card, comprising:

A communication unit to communicate with the outside (figure 2: 26; IC Card);

An information accumulating unit to accumulate data and a program (figure 2: 54; RAM; 56); and

An arithmetic processing unit to perform information processing (figure 2: 52 CPU, Cryptography Accelerator; 62);

Wherein said information accumulating unit stores value data, two or more transfer keys that update the value data, a transfer key identifier used to identify the transfer key currently selected, and that identifies said two or more transfer key (Column 5: lines 27-42; Column 6: lines 60-67; column 7: line 1-5; column 12: lines 1-25);

Wherein if the value of the transfer key identifier, which is received by said communication unit, is newer that of said selection transfer key identifier, and which is equivalent to either a value of said transfer key identifier stored by said information accumulating unit, said arithmetic processing unit updates said selection transfer key identifier to the transfer key identifier received by said

communication unit by performing encryption using the update key on the basis of common-key cryptography (column 7: lines 39-45); and

Wherein said arithmetic processing unit then updates the value data by performing encryption using the transfer key corresponding to the update transfer key identifier on the basis of common-key cryptography (column 7: lines 39-45).

Guthery does not disclose update value data. Akiyama, in analogous art, however, discloses updating transaction and update value data (Figure 15: IC card ledger file). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Guthery to include updating transaction and update value data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an enhanced security of an electronic cashless transaction system, thereby allowing versatile uses of an IC card as an ultimate medium for commercial transactions in general as suggested by Akiyama in (column 4: lines 43-48).

Allowable Subject Matter

14. Claims 2, 4, 6, 7 and 9 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

15. The following is a statement of reasons for the indication of allowable subject matter Smart cards have come into widespread use and are being used instead of magnetic cards and

have distinct advantages that the magnetic cards do not have. To perform valuable transaction settlement processing using Smart cards, illegal coping and tampering with the value must be prevented. This requires the tamper resistance smart card, and communication processing between smart cards which uses encryption.

The disclosed invention provides a settlement terminal that transmits/receives value data between a first smart card that accumulates first value data, a first transfer key used to update the first value data, and an update key used to update the first transfer key, and a second smart card that accumulates second value data, a second transfer key used to update the second value data, and an update key used to update the second transfer key, the settlement terminal comprising: first smart-card read/write means whereby, if the first transfer key differs from the second transfer key, the first transfer key encrypted by use of the update key is received from the first smart card; and second smart-card read/write means for transmitting, to the second smart card, a transfer-key update request requesting that the second transfer key of the second smart card is updated to the first transfer key, said transfer-key update request including the first transfer key encrypted by use of the update key.

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See the notice of reference cited in form PTO-892 for additional prior art.

17. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T-G

Techane Gergiso

Patent Examiner

Art Unit 2137

August 6, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER